

REMARKS

Claims 1-6, 8-18 and 20-25 remain pending in the present application. Claims 1, 11, 15, 20 and 25 are independent claims. Applicant requests reconsideration and allowance in view of the following remarks.

Rejection under 35 U.S.C. § 103(a) based on Fischer, Goodman, Menezes and Nakamura

On pages 2-7, the Action rejects claims 1-6, 8-18 and 20-25 under 35 U.S.C. 103(a) as allegedly being unpatentable over Fischer (U.S. Patent No. 5,001,752) in view of Goodman (U.S. Patent No. 5,001,752), Menzes (Handbook of Applied Cryptography), and Nakamura (U.S. Patent No. 6,457,126). Applicant respectfully traverses this rejection.

For at least the following reasons, Applicant disagrees with the assertions made in the Office Action alleging that the cited references in combination render claim 1 obvious under 35 U.S.C. § 103(a).

Regarding claim 1, the Action states that Fischer fails to teach a system having two separate modes. In addition to not teaching this limitation, Fischer fails to teach using a secure encryption key in a first mode for encryption and test operations and using the secure encryption key in a second mode for timestamping operations.

In FIG. 1, Fischer discloses a processor module 6 coupled to a storage device 8. The storage device stores a secret private key of a public/private key pair (also see Fischer, col. 4, lines 35-38). Fischer does not teach the processor module 6 using the secret private key in a first mode for encryption operations and for test operations and using the key in a second mode in which the secret private key is only used for timestamping operations.

The Action relies on Goodman to overcome the deficiencies of Fischer. However, Goodman, alone or in combination with Fischer, fails to teach the invention as claimed in claim 1.

First, Goodman fails to teach the two different modes as claimed in claim 1. Instead, Goodman teaches an encryption mode and a test mode. If aligned with the modes of claim 1, both the encryption mode and test mode fall under the first mode of claim 1. Goodman does not teach or suggest a second, separate timestamping mode. Therefore, Goodman fails to overcome the deficiency of Fischer.

Further, even if, *arguendo*, Goodman teaches two separate modes, in the two "modes" taught by Goodman, the encryption processor uses a private test key in the test mode, and a separate secure electronic key in the work mode using (see Goodman, col. 5, lines 14-20, col. 5, lines 62-col. 6, line 2, col. 6, lines 55-56, also see col. 7, lines 15-28). Thus, Goodman teaches using separate keys in separate respective "modes". Nowhere does Goodman teach using a secure encryption key in a first mode for encryption and test operations and using the secure encryption key in a second mode for timestamping operations. Specifically, Goodman does not teach that the encryption processor 23 (or 33, 43, 66) using a private test key (or a secure electronic key) in a first mode for encryption operations and for test operations and using the private test key (or the secure electronic key) in a second mode in which the key is only used for timestamping operations. Therefore, Fischer in light of Goodman does not teach all of the claim features.

A person of ordinary skill in the art would not have been motivated to combine Fischer and Goodman to produce the claimed invention, because neither reference, alone or in combination teaches the claimed invention, as conceded in the Action on page 3.

In the Action on page 3, the Action concedes that the combination of Fischer and Goodman fails to teach precluding the processor from performing in the first mode with the same secure encryption key when the secure encryption key has been used to perform a function in the second mode. The Action relies on the session keys as taught by Menezes to teach this limitation.

However, Menezes, alone or in combination with Fischer and Goodman, fails to overcome the deficiencies of Fischer and Goodman. Specifically, Menezes fails to teach using a secure encryption key in a first mode for encryption and test operations and using the secure encryption key in a second mode for timestamping operations. Menezes fails to teach using the same key for a first mode and for a second mode as claimed in claim 1, as conceded on page 4 of

the Action. Therefore, Menezes, alone in combination with Fischer and Goodman, fails to teach or suggest the invention in claim 1.

On page 3 of the Action, the Action concedes that the modified Fischer, Goodman, and Menezes system fails to disclose the same key is used in both modes. The Office (?) states that Nakamura teaches a key used in two modes in col. 15, lines 66 through col. 16, line 5, and col. 17, lines 9-26, and asserts that at the time of the invention it would have been obvious to one skilled in the art to use the same key in both modes of the modified Fischer, Goodman, and Menezes system. Applicant respectfully disagrees with this characterization of Nakamura, and respectfully asserts that Nakamura, alone or in combination with Fischer, Goodman and Menezes, fails to overcome the deficiencies of these references.

Nakamura in fact teaches using **two keys** (e.g. data key K1 and system key K2) in **one of the claimed modes**. See, e.g., Nakamura col. 15, lines 3-33. Nakamura discloses an encryption/decryption operation and test operations (Nakamura, col. 16, line 47). If aligned with the processor modes of claim 1, both of these modes would fall under the first mode as claimed in claims 1, 11, 15, and 20. Nakamura does not teach or discuss a second **timestamping** mode. Applicant respectfully submits that this, or any other Nakamura disclosure fails to teach or reasonably suggest the use of a **single key** in multiple modes, one mode for **test and, encryption, and one mode timestamping**, as set forth in claim 1. At best, Nakamura discloses two keys used in two modes. There is no teaching or suggestion of using the same key for testing operations, encryption operations and timestamping operations.

Again, as previously explained, the only teaching of providing a processor that uses a **single key** in multiple modes for test, encryption, and timestamping operations is found in Applicant's disclosure. Based on the teachings of Fischer and Goodman, assuming, *arguendo*, that there is motivation to combine these references, one of ordinary skill in the art would not modify the references as alleged by the Action. One of ordinary skill in the art might modify the processor module 6 of Fischer to have two modes and use the secret private key of Fischer in the work mode, similar to that of Goodman, and add a test mode to the processor module 6 of Fischer to use the private test key in the test mode, similar to that of Goodman. Thus, assuming that proper motivation to combine could be found, the combined teachings might suggest using separate keys in separate modes. However, this modification does not teach or suggest providing

a processor that uses a **single key** in different operations in different modes. The Action impermissibly relies on Applicant's own disclosure to bridge this gap between the teachings of Fischer in view of Goodman and the claimed invention. Without Applicant's teachings of providing a processor that uses a **single key** in a first mode for encryption and test operations and in a second mode for timestamping operations, one of ordinary skill in the art would not modify the combined teachings of the cited references as stated in the Action to render claim 1 obvious. Thus, the combined teachings of Fischer, Goodman, Menezes, and Nakamura do not teach or suggest the features of claim 1, in contrast with the statements of the Action.

Applicant respectfully submits that the Office has improperly applied individual parts of Goodman, Fischer, Menezes and Nakamura as a mosaic to recreate a facsimile of the invention. It is well known that it is improper to use the claims as a frame, and use individual parts of prior art as a mosaic to recreate a facsimile of the invention. *Interconnect Planning Corp. v. Feil*, 227 USPQ 2d 543, 551 (Fed. Cir. 1985).

Applicant respectfully requests that the Examiner also reconsider the arguments presented in the previous filings, which are not included herein, for brevity. Thus, for at least the reasons stated above, the combined teachings of Fischer, Goodman, Menezes, and Nakamura do not teach or suggest all of the features recited in claim 1. Therefore, the Action does not establish a *prima facie* case of obviousness to reject claim 1 under 35 U.S.C. § 103(a) based on the combined teachings of Goodman, Fischer, Menezes and Nakamura.

Accordingly, claim 1 is allowable over the cited references and allowance thereof is respectfully requested. Claims 2-6 and 8-10, which depend from claim 1, are also in condition for allowance because of their dependence on an allowable claim.

Claim 11 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested. Claims 12-14, which depend from claim 11, are also in condition for allowance because of their dependence on an allowable claim.

Claim 15 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested. Claims 16-18, which depend from claim 15, are also in condition for allowance because of their dependence on an allowable claim.

Claim 20 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested. Claims 21-24, which depend from claim 20, are also in condition for allowance because of their dependence on an allowable claim.

Claim 25 is allowable for reasons analogous to those given for claim 1 and allowance thereof is respectfully requested.

Applicant requests reconsideration and withdrawal of the rejection of claims 1-6, 8-18 and 20-25 under 35 U.S.C. § 103(a) as being unpatentable over Goodman, Fischer, Menezes and Nakamura.

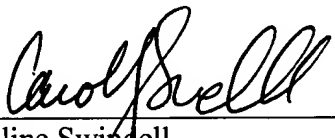
Conclusion

All of the stated grounds of rejection have been properly traversed. Applicant therefore respectfully requests that the Examiner reconsider all presently outstanding rejections and that they be withdrawn. Applicant believes that a full and complete reply has been made to the outstanding Office Action and, as such, the present application is in condition for allowance. If the Examiner believes, for any reason, that personal communication will expedite prosecution of this application, the Examiner is hereby invited to telephone the undersigned at the number provided.

Prompt and favorable consideration of this Amendment is respectfully requested.

Date: July 21, 2006

Respectfully submitted,

By 
Caroline Swindell
Registration No. 56,784
VENABLE LLP
P.O. Box 34385
Washington, DC 20043-9998
(202) 344-4000
(202) 344-8300 (Fax)
Attorney/Agent for Applicant